# Posudek oponenta diplomové práce

**Student:** Jacko Michal, Bc.
**Téma:** Metody klasifikace síťového provozu (id 20238)
**Oponent:** Ovšonka Daniel, Ing., UITS FIT VUT

**1. Náročnost zadání** **průměrně obtížné zadání**

Jedná se o průměrně obtížné zadání experimentálního charakteru. Student musel nastudovat možnosti paralelizace výpočtu metrik TCP toku na GPU s využitím technologie CUDA.

**2. Splnění požadavků zadání** **zadání splněno s drobnými výhradami**

Student částečně diskutuje všechny body zadání. Výhrady mám k splnění bodu 1. zadání, kde nepovažuji popis aktuálních metod a nástrojů za dostatečný, kdeže úplně chybí analýza náročnosti na výpočetní prostředky. Částečné výhrady mám aj vůči splnění bodu 3. zadání, kde student nevykonal žádné porovnaní s jinými nástroji.

**3. Rozsah technické zprávy** **téměř splňuje minimální požadavky**

Technická část má zhruba 40 normostran. Jednotlivé kapitoly jsou poměrně strohé a nevěnují se problematice do dostatečné hloubky spíše jen v obecné rovině.

**4. Prezentační úroveň předložené práce** **50 b. (E)**

Technická zpráva je dobře strukturovaná a jednotlivé kapitoly na sebe logicky navazují. Teoretická část práce je ale zpracovaná značně podprůměrně. Rozsahy jednotlivých kapitol jsou mnohokrát nedostačující, co se projevuje hlavně na analýze aktuálního stavu problematiky a popisu vlastní implementace.

**5. Formální úprava technické zprávy** **60 b. (D)**

Po formální stránce je práce na průměrné úrovní, obsahuje jen minimum pravopisných a typografických chyb (hlavně přetečení textu a jednopísmenové spojky/předložky na konci řádku).

**6. Práce s literaturou** **60 b. (D)**

Práce s literaturou je na standartní úrovni, citované jsou významné články ze zkoumané oblasti. Převzaté části jsou snadno odlišitelné od vlastního přínosu autora. Drobným nedostatkem je zařazení do seznamu literatury aj zdroje odkazující na nástroje a články které s prací souvisí pouze okrajově ([3], [4], [5], [15]).

**7. Realizační výstup** **50 b. (E)**

Realizační výstup je rozporuplný. Student byl schopný navrhnout a implementovat výpočet metrik na GPU tyto metriky ale dále nejsou při klasifikaci používány. Implementované detektory jsou pouze triviální a dali by se použit aj bez výpočtu metrik. Detektory používají na klasifikaci pouze jednoduchý rozhodovací strom. Zdrojové kódy jsou dobře strukturované a přehledné. Jádro výpočtu metrik na GPU pomocí Gaussovi eliminační metody je zřejmě převzato z externích zdrojů bez uvedení reference.

**8. Využitelnost výsledků**

Jedná se o práci kompilačního charakteru, student využívá pouze známe metody analýzy sítového toku. Moduly na výpočet metrik jednotlivých TCP toků by bylo možné použít při dalších experimentech s detekcí anomálii s použitím pokročilejších technik klasifikace. Na druhé straně, navrhnuté detektory jsou prakticky nepoužitelné v praxi nebo při dalším výzkumu.

**9. Otázky k obhajobě**

- Není podle Vás použití No-SQL databáze na uložení vypočtených metrik za kontraproduktivní? Výkonnost No-SQL databáze je obecně nižší přičemž metriky jde jednoduše normalizovat a uložit do relační databáze.

**10. Souhrnné hodnocení** **50 b. dostatečně (E)**

Jedná se o poměrně nevyváženou práci, která je degradována úrovní technické správy, která je místy nedostatečná. Realizační výstup taktéž obsahuje signifikantní nedostatky. Na základe výše uvedeného považuji práci jako celek na hranici dostatečnosti pro diplomovou práci, která se dá hodnotit stupněm **E - dostatečně** jen s výraznými výhradami.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 8. června 2017

.....
podpis